

REMARKS

A. GENERALLY

Claims 1-17 remain in the Application. Claims 1-17 have been amended. No new matter has been added.

B. OBJECTIONS TO THE DISCLOSURE

With respect to the disclosure objection, Applicant respectfully declines to add section headings because the indicated suggestions in 37 C.F.R. § 1.77(b) are not statutorily required for filing a non-provisional patent application under 35 USC § 111(a), but per 37 C.F.R. § 1.51(d) are only guidelines that are suggested for Applicant's use. Thus, the section headings are not mandatory, and in fact when Rule 77 was amended in 1996 (61 FR 42790, Aug. 19, 1996), Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks, stated in the Official Gazette:

"Section 1.77 is permissive rather than mandatory. ... 1.77 merely expresses the Office's preference for the arrangement of the application elements. The Office may advise an applicant that the application does not comply with the format set forth in 1.77, and suggest this format for the applicant's consideration; however, the Office will not require any application to comply with the format set forth in 1.77."

In view of the above, Applicant respectfully declines to amend the specification to include the suggested section headings, and respectfully request that this objection be withdrawn.

C. CLAIM OBJECTIONS

Claim 11 has been objected to on the grounds that it is a method claim that appears to depend from an apparatus claim. Applicant notes that this form of claim is not inherently objectionable:

2173.05(f) Reference to Limitations in Another Claim

A claim which makes reference to a preceding claim to define a limitation is an acceptable claim construction which should not necessarily be rejected as improper or confusing under 35 U.S.C. 112, second paragraph. For example, claims which read: "The product produced by the method of claim 1." or "A method of producing ethanol comprising contacting amylose with the culture of claim 1 under the following conditions" are not indefinite under 35 U.S.C. 112, second paragraph, merely because of the reference to another claim. See also Ex parte Porter, 25 USPQ2d 1144 (Bd. Pat. App. & Inter. 1992) where reference to "the nozzle of claim 7" in a method claim was held to comply with 35 U.S.C. 112, second paragraph. However, where the format of making

reference to limitations recited in another claim results in confusion, then a rejection would be proper under 35 U.S.C. 112, second paragraph.

Applicant has elected to amend claim 11 so as to place it in the form of an independent claim.

Claim 17 (a method claim) as examined claimed dependency from claim 10 (an apparatus claim). Applicant has amended claim 17 to depend from claim 11.

Based on the foregoing, Applicant requests that the objections to claims 11 and 17 be withdrawn.

D. CLAIMS REJECTIONS

1. Claim Rejections Pursuant to 35 U.S.C. §112

Claims 1, 3, 7, 8 and 15 have been rejected pursuant to 35 U.S.C. §112(¶2) as failing to specifically point out what is being claimed. In particular, the Office Action asserts that specific limitations recited in the claims lack antecedents thereby rendering them unclear. Based on the amendment of these claims, Applicant requests that this rejection be withdrawn.

2. Claim Rejections Pursuant to 35 U.S.C. § 102(b)

Claims 1 and 4 have been rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,261,003 issued to Matsui (hereinafter, "Matsui").

Claim 1 (as amended) recites the following limitations:

1. (Currently Amended) A processor for encrypting and decrypting data comprising:
a control device is connected to at least one encryption/decryption means via at least one communication means, wherein the control device comprises a memory and at least one key input that receives an initial key from a source other than the key generation means, and

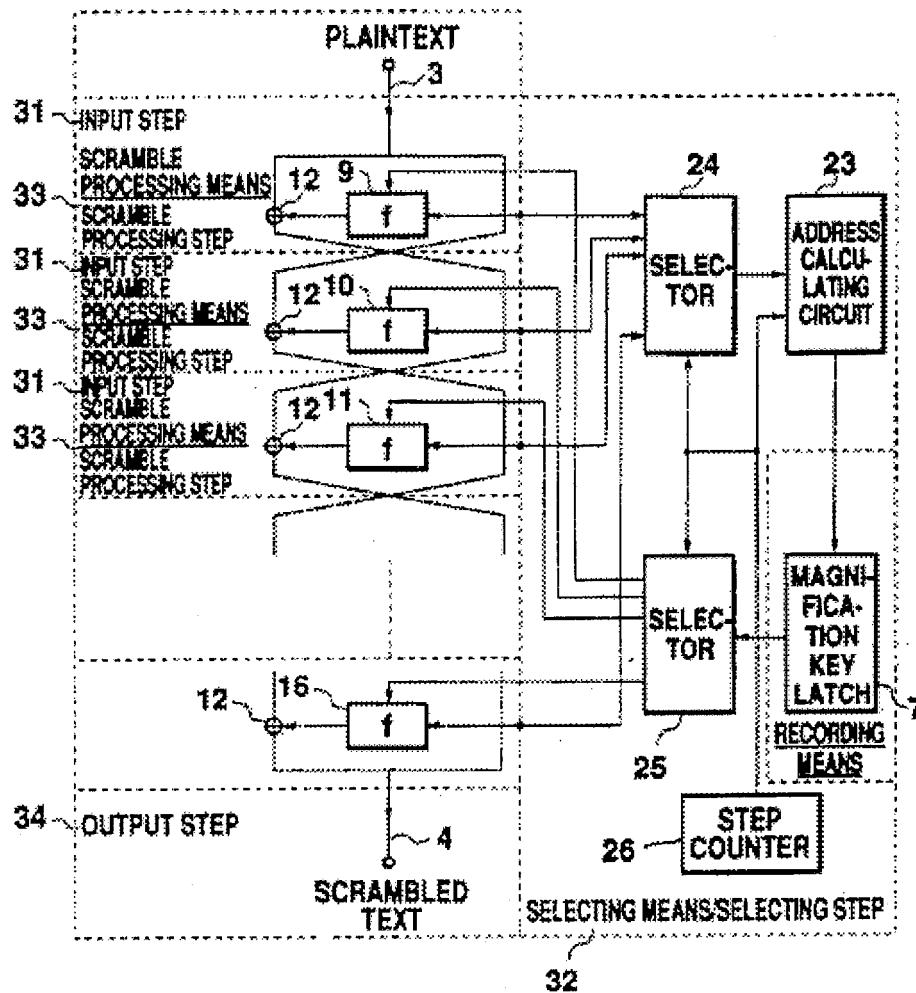
at least one round key generation means connected to the control device via at least one further communication means, wherein the round key generation means receives a data word from the control device for calculating at least one round key and transfers the at least one round key to the memory of the storage device;

wherein the at least one encryption/decryption means comprises at least one external data input for receiving the data, an input for receiving the at least one round key from the memory of the control device, and at least one external data output for outputting data processed with the at least one round key, and

wherein the at least one encryption/decryption means and the at least one round key generation means communicate solely via the control device.

The Office Action asserts that Matsui discloses an encryption/decryption means that is decoupled from a round key generation means. Applicant respectfully disagrees.

Figure 1 of Matsui illustrates a scrambling system as follows:



Applicant respectfully submits that Matsui teaches a communication system in which a pre-stored key is selected from storage based on an address that is calculated from input plain text data. The selector and the key latch do not generate a key as recited in claim 1 (as amended). Rather, a key that is pre-stored in key latch 7 is selected. Thus, Matsui does not teach the limitation, "wherein the round key generation means receives a data word from the control device for calculating at least one round key and transfers the at least one round key to the memory of the storage device."

The Office Action maps the illustrated elements 23, 24 and 25 to the recited control device. Elements 23 and 7 are mapped to the recited round key generation means. The suggested mapping of element 23 to both the recited control device and the recited key generation means places the key generation means in direct communication with the

encryption/decryption means. This mapping thus violates the limitation, “wherein the at least one encryption/decryption means and the at least one round key generation means communicate solely via the control device” as recited in claim 1 (as amended). Applicant respectfully submits that the mapping of Matsui to the structures of claim 1 (as amended) as suggested in the Office Action is inconsistent with claim 1 (as amended) read as a whole. Based on the foregoing, Applicant submits that Matsui does not teach the control device and the round key generation means recited in claim 1 (as amended).

The Office Action further asserts that the illustrated connection between key latch 7 and selector 25 discloses the recited external key input of the control device and that the connections of the selector 25 to the various processing blocks (9) disclose the external data input to the recited encryption/decryption means.

Claim 1 (as amended) recites, “wherein the control device comprises … at least one external key input that receives an initial key from a source other than the key generation means.” However, according to the Office Action, selector 25 is part of the claimed control device and key latch 7 is part of the claimed round key generating means. Thus, the connection cited in the Office Action does not teach this limitation as currently amended.

The illustrated connections of the selector 25 to the various processing blocks (9) carry the key selected from key latch 7. The preamble of claim 1 (as amended) is directed to “a processor for encrypting and decrypting data.” Thus, the data of claim 1 is not key data. Claim 1 (as amended) recites, “wherein the at least one encryption/decryption means comprises at least one external data input for receiving the data....” The cited connections do not represent an external data input for receiving “the data.”

Based on the foregoing, Applicant respectfully submits that claim 1 is not anticipated by Matsui.

Claim 4 (as amended) depends from claim 1 (as amended) and recites all of the limitations of that base claim. Claim 4 thus recites limitations that are not taught by Matsui and is, therefore, not anticipated by that reference.

3. Claim Rejections Pursuant to 35 U.S.C. § 103(a)

Claims 2-3 and 6-7 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of a publication by John L. Hennessy and David A. Patterson entitled, "Computer Architecture: A Quantitative Approach," 2nd Ed. Morgan Kaufmann, January 1996 (hereinafter, "Hennessy-Patterson").

Claims 2-3 and 6-7 as currently listed depend from claim 1 (as amended) and recite all of the limitations of that base claim. Applicant has demonstrated that Matsui does not teach all of the limitations of claim 1 (as amended). The Office Action does suggest that Hennessy-Patterson cures the deficiencies of Matsui identified in the discussion of claim 1 (as amended) above. Thus, claims 2-3 and 6-7 recite limitations not taught by the combination of Matsui and Hennessy-Patterson and are patentable over the cited prior art.

Claim 5 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of U.S. Patent 5,919,251 issued to Tran (hereinafter, "Tran"). Claim 5 as currently listed depends from claim 1 (as amended) and recites all of the limitations of that base claim. Applicant has demonstrated that Matsui does not teach all of the limitations of claim 1 (as amended). The Office Action does not suggest that Tran cures the deficiencies of Matsui identified in the discussion of claim 1 (as amended) above. Thus, claim 5 (as currently listed) recites limitations not taught by the combination of Matsui and Tran and is patentable over the cited prior art.

Claims 8, 9, 11, 15 and 16 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of U.S. Patent Application 2002/0021802 filed by Muratani et al. (hereinafter, "Muratani").

Claims 8 and 9 as currently listed depend from claim 1 (as amended) and recite all of the limitations of that base claim. Applicant has demonstrated that Matsui does not teach all of the limitations of claim 1 (as amended). The Office Action does not suggest that Muratani cures the deficiencies of Matsui identified in the discussion of claim 1 (as amended) set forth above. Thus, claims 8 and 9 (as currently listed) recite limitations not taught by the combination of Matsui and Muratani and are patentable over the cited prior art.

Claim 11 (as amended) recites limitations similar in scope to claim 1 (as amended). The Office Action asserts that Matsui teaches the limitations of claim 11 with the exception of the recited recursive key generation step. The recursive key step is said to be disclosed by Muratani.

According to step (a) of claim 11 (as amended), “at least one initial key is read into a control device, wherein the at least one initial key is obtained from a source other than a round key generation means.” The Office Action points to the provision of a key by key latch 7 to selector 25 as meeting this step. However, according to the Office Action, key latch 7 is a part of the round key generation means recited in claim 11. Thus, Matsui does not teach this limitation of claim 11 (as amended).

According to step (c) of claim 11 (as amended), “at least one data word needed to calculate at least one round key is read from at least one storage means of the control device and transferred to at least one round key generation means.” The Office Action asserts that this step is met by the disclosure of Matsui inputting portions of plaintext data into the address calculating circuit 23. Applicant respectfully submits that the disclosed functions of address calculating circuit 23 do not include calculating a round key.

According to step (d) of claim 11 (as amended), “at least one round key is calculated recursively on the basis of the at least one data word by means of the at least one round key generation means, transferred to the control device and stored in the at least one storage means.” The Office Action asserts that Matsui discloses a key generation step (d) as recited in claim 11 (as amended). Applicant respectfully disagrees. Matsui teaches a communication system in which a pre-stored key is selected from storage based on an address that is calculated from input plain text data. The selector and the key latch do not generate a key as recited in claim 11 (as amended). Rather, a key that is pre-stored in key latch 7 is selected. The computation of an address and the selection of a key based on that address do not teach the limitations of steps (c) and (d) in which a data word is used to compute a round key.

Muratani is not cited as overcoming the deficiencies of Matsui discussed above. Based on the foregoing, Applicant submits that claim 11 (as amended) is patentable over the combination of Matsui and Muratani.

Claims 15 and 16 as currently listed depend from claim 11 (as amended) and recite all of the limitations of that base claim. Applicant has demonstrated that Matsui does not teach all of the limitations of claim 11 (as amended). The Office Action does not suggest that Muratani cures the deficiencies of Matsui identified in the discussion of claim 11 (as amended) set forth above. Thus, claims 15 and 16 (as currently listed) recite limitations not taught by the combination of Matsui and Muratani and are patentable over the cited prior art.

Claim 10 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of U.S. Patent Application 2003/0202658 filed by Verbauwhede (hereinafter, "Verbauwhede"). Claim 10 (as amended) depends from claim 1 and recites all of the limitations of that base claim. Verbauwhede is cited as disclosing that the processor is an AES coprocessor but is not cited as overcoming the deficiencies of Matsui identified in the discussion of claim 1 (as amended) set forth above. Based on the foregoing, claim 10 (as amended) is patentable over the combination of Matsui and Verbauwhede.

Claims 12 and 13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani in further view of Hennessy-Patterson. Claims 12 (as amended) and 13 (as amended) depend from claim 11 (as amended) and recite all of the limitations of that base claim. Claim 11 (as amended) has been shown to be patentable over the combination of Matsui and Muratani. Hennessy-Patterson has been cited as teaching the additional limitations of claims 12 (as amended) and 13 (as amended) but has not be cited as overcoming the deficiencies of the combination of Matsui and Muratani identified in the discussion of claim 11 (as amended) set forth above. Based on the foregoing, claims 12 (as amended) and 13 (as amended) are patentable over the combination of Matsui, Muratani and Hennessy-Patterson.

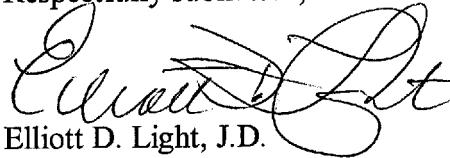
Claim 14 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani et al. and Tran. Claim 14 depends from claim 11 (as amended) and recites all of the limitations of that base claim. Claim 11 (as amended) has been shown to be patentable over Matsui and Muratani. Tran has been cited as teaching the additional limitations of claim 14 (as amended) but has not been cited as overcoming the deficiencies of the combination of Matsui and Muratani identified in the discussion of claim 11 (as amended) set forth above. Based on the foregoing, claim 14 (as amended) is patentable over the combination of Matsui, Muratani and Tran.

Claim 17 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of U.S. Patent Application 2003/0202658 filed by Verbauwhede. Claim 17 (as amended) depends from claim 11 and recites all of the limitations of that base claim. Verbauwhede is cited as disclosing that the processor is an AES coprocessor but is not cited as overcoming the deficiencies of the combination of Matsui and Muratani identified in the discussion of claim 11 (as amended) set forth above. Based on the foregoing, claim 17 (as amended) is patentable over the combination of Matsui, Muratani and Verbauwhede.

E. CONCLUSION

Applicant respectfully submits that the claims as currently listed are in condition for allowance. Applicant requests that this response be entered and that the current rejections of the claims and objections to the disclosure now pending in this application be withdrawn in view of the above amendments, remarks and arguments.

Respectfully submitted,



Elliott D. Light, J.D.

Registration No. 51,948

Jon L. Roberts, Ph.D., J.D.

Registration No. 31,293

Roberts Mardula & Wertheim, LLC

11800 Sunrise Valley Drive, Suite 1000

Reston, VA 20191-5302

(703) 391-2900